IN THE U.S. DISTRICT COURT FOR MARYLAND
SOUTHERN DIVISION

Beyond Systems, Inc. **9501 Anchorage Place** **Bethesda, MD 20817** **Plaintiff,** **v.** **World Avenue U.S.A., LLC** **successor by merger to Niutech, LLC** **dba "TheUseful"** **1613 NW 136th Avenue, Suite 100** **Sunrise, FL 33323** **and** **World Avenue Holdings, LLC** **1613 NW 136th Avenue, Suite 100** **Sunrise, FL 33323** **Serve: Corpdirect Agents, Inc.** **515 East Park Avenue** **Tallahassee, Florida 32301** **Niuniu Ji** **1613 NW 136th Avenue, Suite 100** **Sunrise, FL 33323** **and** **John Does 1-20** **Defendants.**	*	**Case No. 8:08-cv-00921-PJM** **AMENDED COMPLAINT AND JURY DEMAND**

AMENDED COMPLAINT

Plaintiff BEYOND SYSTEMS, INC. ("BSI") files this Amended Complaint against Defendants WORLD AVENUE U.S.A., LLC ("WAUSA") dba "TheUseful," successor by merger to Niutech, LLC; WORLD AVENUE HOLDINGS, LLC ("WAH"), NIUNIU JI ("JI"), and JOHN DOES 1 THROUGH 20, (collectively, "DEFENDANTS").

I. INTRODUCTION

1. This action arises from the transmission of one or more unsolicited, commercial electronic mail messages (hereinafter, "email") to the Plaintiff BSI in violation of the Maryland Commercial Electronic Mail Act. See Maryland Code Ann., Commercial Law §14-3001 et seq. (hereinafter, "MD-CEMA") and the Florida Electronic Mail Communications Act, Florida Statutes Annotated § 668.60 et seq. (hereinafter, "FL-CEMA").

II. THE PARTIES

2. BSI is a corporation formed under the laws of the State of Maryland, and maintaining its principal offices in Montgomery County, Maryland. BSI is an "interactive computer service provider" as defined under the MD-CEMA and an "interactive computer service" as defined under FL-CEMA -- providing computer services and Internet access to multiple users simultaneously. Providers of Internet access and services, such as BSI, are known as Internet Service Providers ("ISP").

3. Defendant WAUSA is a limited liability company formed under the laws of Delaware, and maintaining its principal business offices in Sunrise, Florida. As a result of a

merger, WAUSA is the successor in interest to, and has assumed the liabilities of, NIUTECH, LLC. WAUSA conducts business on a regular basis in Maryland.

4. Defendant WAH is a limited liability company formed under the laws of Florida, and maintaining its principal offices in Sunrise, Florida. WAH conducts business on a regular basis in Maryland.

5. Defendant JI is an individual residing in Sunrise, Florida. JI conducts business on a regular basis in Maryland. Ji owns a controlling interest in, and exercises control over the daily activities of, WAH and WAUSA and other entities through which he conducts business with and for WAH and WAUSA, and conducts business on a regular basis in Maryland.

6. JI executed articles of merger as the sole representative for WAUSA and NIUTECH, LLC. JI, and the entities controlled by JI, including WAUSA, WAH and some of the JOHN DOE defendants to be identified specifically when their true names are known, are referred to hereinafter in this Amended Complaint collectively as "WORLD AVENUE."

7. Defendants JOHN DOES 1 THROUGH 20 are persons, organizations, and/or corporations who, along with the other Defendants, initiated, conspired in the initiation, or assisted in the transmission of the emails at issue. The names, "JOHN DOES 1 THROUGH 20" are fictitious. Plaintiff is now unaware of the true names of these defendants and will seek leave to file another Amended Complaint alleging the true names of the John Doe Defendants once ascertained. (Collectively, all the defendants in the present case will hereinafter be referred to as "DEFENDANTS").

III. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over the claims in this action pursuant to 28 U.S.C. § 1332 (diversity jurisdiction). Plaintiff is a resident of Maryland. Defendant WAUSA is a limited liability company formed and existing under the laws of the State of Delaware; Defendant WAH is a limited liability company formed and existing under the laws of the State of Florida, and Defendant JI is a resident of the State of Florida and regularly conducts business in the State of Maryland. Plaintiff claims more than $75,000 in damages, exclusive of costs, interest and attorney's fees.

9. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a)(2), (3) and (c), as the events giving rise to the present claims occurred in the District of Maryland.

IV. UNSOLICITED, COMMERCIAL EMAIL

A. Unsolicited Commercial Email Unfairly Shifts the Cost Burden from Sender to Recipient.

10. Unsolicited advertising over the Internet is often referred to as "unsolicited commercial email" or "UCE," "unsolicited bulk email," "junk email," or "Spam." See Beyond Systems, Inc. v. Realtime Gaming Holding Co., LLC, 388 Md. 1, 16 n. 12; 878 A.2d 567, 576 n.12 (quoting State v. Heckel, 143 Wn.2d 824, 24 P.3d 404, 406 n.1 (Wash. 2001)).

11. The MD-CEMA defines "Commercial electronic mail" as "electronic mail that advertises real property, goods, or services for sale or lease." See Maryland Code Ann., Commercial Law §14-3001(b)(1).

12. The MD-CEMA prohibits the initiation of a transmission, any conspiracy to initiate a transmission, or any assistance of a transmission of commercial electronic mail that is

sent from a computer in the State or is sent to an email address is held by a resident of the State and that (i) uses a third party's Internet domain name or email address without the permission of the third party; (ii) contains false or misleading information about the origin of the transmission path of the commercial email; or (iii) contains false or misleading information in the subject line that has the capacity, tendency, or effect of deceiving the recipient. See Maryland Code Ann., Commercial Law §14-3002(b).

13. The FL-CEMA defines an "Unsolicited commercial electronic mail message" as "any commercial electronic mail message that is not a transactional or relationship message and is sent to a recipient without the recipient's affirmative or implied consent." See Florida Statutes Annotated § 668.602(14).

14. The State of Florida prohibits the initiation or the assistance in the transmission of an unsolicited commercial electronic mail from a computer in the State or to an email address held by a resident of the State that : (a) uses a third party's Internet domain name without permission; (b) contains falsified or missing routing information or otherwise misrepresents, falsifies, or obscures any information in identifying the point of origin or the transmission path of the unsolicited commercial email message; (c) contains false or misleading information in the subject line; (d) or contains false or deceptive information in the body of the message which is designed and intended to cause damage to the receiving device of an addressee or of another recipient of the message. See Florida Statutes Annotated § 668.603.

15. Spam poses a serious threat to electronic communication over the Internet for consumers and businesses because the messages are rife with deception and fraud. In 2003, the

Federal Trade Commission accurately estimated that about two-thirds of the spam analyzed contained likely false claims in the "From:" line, "Subject:" line, or message text and nearly 85% of the spam analyzed were deceptive on their face or advertised an illegitimate product. See "National Do Not Email Registry: A Report to Congress." FTC, June 2004, p. 1 & n. 2, available at http://www.ftc.gov/reports/dneregistry/report.pdf (last visited 12/21/08).

16. The FTC accurately stated the problem of Spam begins with the uniformly held understanding that "spammers are essentially anonymous. The current email system enables spammers to hide their tracks and thereby evade ISPs' anti-spam filters and law enforcement." See id., p. 1 & section III (pp. 3-13).

17. In 2003, Congress accurately found that Spam accounted for over half of all electronic mail traffic, up from an estimated 7 percent in 2001. See 15 USC § 7701(a)(2) (2003) (CAN-SPAM Act). By 2007, notwithstanding the passage of the federal CAN-SPAM Act, the amount of spam had risen to an estimated ninety to ninety-five percent of all email traffic. See Exhibit 12, BARRACUDA NETWORKS, BARRACUDA NETWORKS SPAM REPORT at 4 (2007).

18. Such an enormous volume of unsolicited and unwanted email traffic places a tremendous strain on resources, especially on private Internet Service Providers such as BSI. To maintain the same level of service to its clients, ISP's must purchase more equipment, purchase additional software, and hire more staff to handle the overwhelming volume of unsolicited and unwanted email traffic to maintain the same level of service to its clients. These additional maintenance costs are eventually passed on to ISP customers – both consumers and businesses – in the form of higher costs and higher monthly access fees.

19. In addition, recipients of unwanted spam often are required to bear additional costs for accessing their own email accounts when they connect remotely to their accounts using a network that charges for access on a per message or a per minute basis, which may occur when an individual uses a wireless network at a hotel, business, or residence.

20. Spam represents an unwanted and non-consensual trespass by spammers into the email accounts and computers of recipients. The flood of Spam can obscure legitimate email messages, which can be mistakenly filtered out as Spam, while deceiving recipients into opening an unsolicited email message disguised to appear legitimate. In addition, Spam can actually prevent the delivery of legitimate email to a recipient by occupying valuable space in the computer's memory, impairing computer performance, or even rendering equipment inoperable.

21. Most Spam contains or advertises offensive, fraudulent, and/or unlawful content such as pornography, prescription drugs, counterfeit software, counterfeit merchandise, bogus university degrees, fake gifts or pyramid schemes, while delivering and sometimes installing malicious viruses, spyware, or other software into the recipient's computer without their knowledge.

B. Recent Litigation.

22. On November 21, 2008, United States District Court Judge Fogel awarded the popular social networking site Facebook $ 873 million in damages from defendants Adam Guerbuez, a Canadian citizen, and his Internet marketing company, Atlantis Capital Blue. After four months of litigation, the Court found that Guerbuez sent more than 4 million spam to subscribers of the website Facebook. These Spam contained advertisements for products such as

marijuana, male enhancement pills, and sexually oriented material. Defendants were allegedly able to complete the conspiracy by stealing logon names and passwords, and utilizing third parties to transmit the messages. See Exhibit 13, Order, Facebook, Inc. v. Guerbuez, et al., Case No. CO8003889 HRL (U.S. District Court, Northern District of California, November 10, 2008).

23. On July 15, 2008, Adam Vitale of Brooklyn, New York was sentenced to 30 months imprisonment for his role in a conspiracy to send unsolicited commercial email over the Internet to nearly 1.2 million subscribers of America Online during a six-day period in August 2005. In addition, Vitale was required to forfeit $ 183,000 in proceeds of his criminal activity. According to Vitale's statements at sentencing, the defendant admitted to sending the spam emails in a manner that deliberately obscured the origin of the emails, concealed defendant's identity, and prevented recipients from tracing the spam and stopping it. See Exhibit 14, USDOJ Press Release: "Brooklyn Man Sentenced to 30 months in Prison in Massive AOL Spam Scheme."

24. On October 12, 2007, the United States District Court for the District of Arizona sentenced defendants Jeffrey Kilbride and James Schaffer to more than five years in prison for organizing and running an international spamming business that grossed over $ 1 million. The federal jury found defendants guilty of at least two counts of sending Spam using falsified header information and domain names registered with materially false information. Defendants admitted to earning a commission for each person they caused to subscribe to one of these web sites. Defendants eventually moved their servers and equipment to Amsterdam, where they re-routed their Spam to appear as if the messages originated abroad, when the messages were

actually being sent from Phoenix, Arizona. See Exhibit 15, USDOJ Press Release, October 12, 2007: "Two Men Sentenced For Running International Pornographic Spamming Business."

25. Online advertiser ValueClick, Inc. paid a record $ 2.9 million to settle Federal Trade Commission ("FTC") charges that its advertising claims and emails were deceptive and violated federal law. The FTC alleged that ValueClick and its subsidiary Hi-Speed Media used deceptive emails, banner ads and pop-up advertisements to drive consumers to its websites. The emails and online advertisements claimed that consumers were eligible for "free" gifts, including laptops, iPods, and high-value gift cards. However, when consumers responded to the advertisements, the advertised items were not free and viewers were required to participate at their own expense to receive the promised "free" merchandise. See Exhibit 16A, FTC Press Release: "ValueClick to Pay $ 2.9 Million to Settle FTC Charges."

26. Online advertiser Adteractive, Inc., agreed to pay a $ 650,000 civil penalty to settle FTC charges that it failed to disclose to consumers that they had to spend money to receive the "Free Gifts" advertised in its emails and websites. According to the FTC, Adteractive dba FreeGiftWorld.com and SamplePromotionsGroup.com, used deceptive spam and online advertising to lure consumers to its websites. The emails and online advertisements included inducements such as "Keep this Flat-Screen TV," and "Congratulations! Claim Your Choice of Sony, HP or Gateway Laptop." The FTC alleged that Adteractive lured customers to its websites using the promises of "Free" merchandise. However, customers desiring to claim their free merchandise were instead led through a maze of expensive and burdensome third-party offers.

See Exhibit 16B, FTC, "Major Online Advertiser Settles FTC Charges. "Free" Gifts Weren't Free; Settlement Calls for $650,000 Civil Penalty," Nov. 28, 2007.

V. FACTUAL BACKGROUND

A. PLAINTIFF BEYOND SYSTEMS, INC.

27. Under the Maryland Code, BSI is an "[i]nteractive computer service provider" and under the Florida Code is an "[i]nteractive computer service." BSI is also an information service, system, and software provider enabling multiple users to access computer servers and a variety of services simultaneously.

28. BSI owns, operates, and maintains its computers and other equipment from its multiple offices in Maryland. As part of its services to clients, BSI operates specialized computers with a dedicated connection to the Internet ("servers") that process email messages and otherwise support its email services to multiple users at the same time.

B. WORLD AVENUE

29. JI, and the entities controlled by JI, including WAUSA, WAH and some of the JOHN DOE defendants who initiated, transmitted, conspired to transmit, or assisted in the transmission of Spam with JI and his companies in the events alleged herein, are referred to hereinafter as "WORLD AVENUE." See www.TheUseful.com.

30. WORLD AVENUE has conducted business under many trade names, including those compiled by the Florida Attorney General. See Exhibit 17, "News Release: Internet Company Sued for Deceptive Advertisements of "Free" Gifts." pp. 1-2.

31. The Better Business Bureau of Southeast Florida has also identified accurate information about NIUTECH, LLC, one of JI's companies and which later merged into WAUSA, listing various trade names, fictitious names, and domain names of Niutech, several of which appear in the emails at issue in this case. See Exhibit 18, pp. 1-2.

32. Exhibit 19 accurately depicts a San Francisco Chronicle article connecting "theUseful," a name that appears frequently in the emails at issue in this case, to WORLD AVENUE.

33. Exhibit 20 shows the "Ripoff Report" for WORLD AVENUE, and accurately lists various Uniform Resource Locators (or "URL's") and fictitious business names that the company uses, several of which appear in the emails at issue in this case.

1. Highly-Incentivized Lead Generation Business Model.

34. WORLD AVENUE is a large-volume participant in the highly incentivized lead generation industry. See Exhibit 21; see also Exhibit 22A. (http://www.theuseful.com/site/aboutus.html last visited December 21, 2008).

35. WORLD AVENUE is a decentralized, online advertiser and marketer that generates business leads for its clients by hiring third party "affiliates" and/or "publishers" to drive traffic to its various websites and encouraging users to divulge their personal identifying information. WORLD AVENUE is paid by its clients on a Cost Per Action basis ("CPA"). See Exhibit 21; see also Exhibit 22B.

36. In the emails at issue in this case, WORLD AVENUE targeted BSI'S personal information using Spam containing false and misleading claims and identifying information.

37. For example, the most common identifier among the emails BSI received from Defendants promoted the trade name or domain name "Superbrewards." See Exhibit 23 (nearly 17,500 occurrences).

38. In thousands of emails that Plaintiff received, WORLD AVENUE promoted the website located at the domain name "Superbrewards.com" using the promise of a "free laptop" or otherwise "Complimentary Laptop Computer." See Exhibit 24.

39. Once at the website advertising the free product or merchandise, the consumer arrives at a landing page that is owned and operated by WORLD AVENUE. In order to collect the "free" gift, the consumer must provide personal information (name, address, email, credit card information) into a form.

40. Once on the registration or survey path to qualify for the "free" gift, WORLD AVENUE required that the customer sign up for several different additional offers in order to qualify for the free item.

41. However, as the investigators from the Florida Attorney General accurately noted, neither the "Program Details" nor "Terms and Conditions" sections found on WORLD AVENUE's websites associated with the "free" offers clearly disclosed important caveats to the promotions. See Exhibit 17, p.1.

42. Rather, the Attorney General's Office accurately noted that WORLD AVENUE's disclaimers on its "free gift" or "free offer" websites should have stated that "every 'free' gift required the consumer to make one or more cash purchases, that the combined dollar amount of

purchases required to receive the gift could exceed the retail value of the 'free' gift" and that the "total cost necessary to obtain the 'free' gift should have also been disclosed." See id., p. 1.

43. WORLD AVENUE then harvests the unsuspecting consumer's personal information to sell as a "lead."

44. As the FTC has accurately noted, a list of active email addresses (not to mention street names and credit card numbers) would be a virtual "goldmine" for spammers and marketers alike. Because there is no universal working directory of email addresses that are "born private," spammers cannot readily identify valid email addresses. See Exhibit 22B.

2. WORLD AVENUE Employs Third Party Marketing Agents to Send Spam on its Behalf

45. WORLD AVENUE contracts with marketing agents ("affiliates" or "publishers") to send unlawful spam on its behalf advertising its various websites. According to its Vice-President and General Counsel Homer Appleby, "The Useful is an Internet marketing company that promotes products and/or services to the consuming public through third party affiliate networks and e-mail marketing companies." Exhibit 25.

46. According to its website, WORLD AVENUE describes itself as a "Web-based marketing and technology company" and "[O]ne of the largest media buyers on the Internet" generating "3 million leads each month." See Exhibit 22A.

47. WORLD AVENUE provides the following services for its clients: display/web advertising, lead generation marketing, email marketing, search engine marketing, and affiliate marketing. See id.

3. WORLD AVENUE Conducts Business Using Fictitious and/or Assumed Names to Conceal Its Identity.

48. WORLD AVENUE conducts business using a number of fictitious or assumed names, most of which are not registered to do business in the State of Maryland or Florida.

49. WORLD AVENUE conducts business under hundreds of alternative domain names and using identities not registered with the State of Maryland or Florida.

50. By law, domain name registrars are required to keep and maintain a list of registration and contact information for each domain name it registers. This information is available through a collectively maintained database known as "Whois." See "Internet Management: Prevalence of False Contact Information for Registered Domain Names." p. 23. GAO Report to the Subcommittee on Courts, the Internet, and Intellectual Property, House of Representatives, November 2005, available at http://www.gao.gov/new.items/d06165.pdf (last visited 12/21/08).

51. Exhibit 26, shows true and correct copies of Whois queries and the results for a sampling of the search terms listed in Exhibit 23, which appear in some of the emails at issue :

ConsumerIncentivePromotions.com – 13900 Jog Road, Suite 203-251, Delray Beach, FL
eMarketResearchGroup.com – 14545 J Military Trail #189, Delray Beach, FL
MyChoiceRewards.com – 14545 J Military Trail #189, Delray Beach, FL
MyPremiumRewards.com – 123 N. Congress Ave. #351, Boynton Beach, FL
NationalSurveyPanel.com – 13900 Jog Road, Suite 203-251, Delray Beach, FL
YourSmartRewards.com – 123 N. Congress Ave. #351, Boynton Beach, FL
SuperbRewards.com – 123 N. Congress Ave. #351, Boynton Beach, FL
ExclusiveGiftCards.com -- 13762 W. SR. 84, Suite 612, Davie, FL 33325

52. Each of the domain names listed above, and the websites hosted at the Uniform Resource Locator addresses or ("URL's"), belong to WORLD AVENUE.

53. The "Terms and Conditions" hyperlinks of the websites listed above are identical in content, form, and trade dress, having the same colors, fonts, and text.

54. The websites listed above are maintained and operated by a company called "Net Radiance", which is referenced in the "Terms and Conditions" section of each of these websites. Exhibit 27 shows true and correct copies of these Terms and Conditions.

55. According to the Florida Secretary of State, Net Radiance LLC is an inactive limited liability company, owned by Niupercent, Inc. Exhibit 28 shows a true and correct copy of registration information regarding Net Radiance LLC from the Florida Secretary of State.

56. Niupercent, Inc. owns WAH. Exhibit 29 shows a true and correct copy of information on World Avenue Holdings LLC from the Florida Secretary of State. World Avenue Holdings LLC, in turn, owns Defendant World Avenue U.S.A. LLC. Exhibit 30.

57. Links on the *SuperbRewards.com* website redirect to *TheUseful.com*, and images appearing on the *SuperbRewards.com* website are actually hosted on *TheUseful.com*. Exhibit 31 shows a true and correct copy of the image properties of an image appearing on *SuperbRewards.com*.

58. In June 2007, the *San Francisco Chronicle* published an article accurately describing WORLD AVENUE's tangled web of corporate ownership, as well as the corporate interrelationships between the entities in that web. See Exhibit 19.

4. WORLD AVENUE is Non-Compliant with Advertising Laws and Ethical Guidelines.

59. In August 2007, the Florida Attorney General sued WORLD AVENUE for its false advertising and deceptive business practices stemming from the company's Internet

marketing practices, including the use of spam in the manner alleged in this Amended Complaint See Exhibit 17, Office of the Attorney General of Florida: "Internet Company Sued for Deceptive Advertisements of "Free" Gifts."

60. In January 2008, WORLD AVENUE settled the lawsuit with the State of Florida for $ 1 Million. See press release, McCollum's CyberFraud Task Force Reaches $1 Million Agreement with Company over Internet Marketing Guidelines. See Exhibit 32.

61. In August 2007, the Direct Marketing Association published an accurate list of advertisers who were not in compliance with its Guidelines for Ethical Business Practice. This list included the website "ExclusiveGiftCards.com," which is operated by WORLD AVENUE and which uses the same operating address and telephone numbers as the call centers listed for the domain names above. This information is confirmed by the Florida Secretary of State. See Exhibit 33, "DMA Ethics Committees Call Attention to Non-Compliant Companies."

C. THE EMAILS AT ISSUE

62. Between July 20, 2004 and September 3, 2005, Plaintiff received on its computer servers in Maryland over 68,000 commercial electronic mail messages promoting products or services offered by World Avenue and its agents. Since July 3, 2005 Plaintiff has received thousands of additional emails from WORLD AVENUE.

63. As used herein, the term, "EMAILS AT ISSUE" means the unsolicited commercial emails that Plaintiff received from WORLD AVENUE, including all emails received up to the date of the entry of any final, non-appealable judgment. .

64. BSI did not solicit or opt-in to receive any of the EMAILS AT ISSUE. Plaintiff gave no direct or indirect consent to receive commercial email from Defendants, and had no business relationship with Defendants, its affiliates, or agents.

65. Some of the EMAILS AT ISSUE are attached to the original Complaint as Documents 1-2, 1-3, 1-4 and 1-5, and are reproduced and attached hereto as Exhibit 34A, 34B, 34C, and 34D.

66. Between July 20, 2004 and September 3, 2005, BSI received at least 68,300 emails from DEFENDANTS. Of those emails, BSI received 61,543 emails between April 11, 2005 and September 3, 2005.

67. The 68,300 EMAILS AT ISSUE to date promote WORLD AVENUE's numerous trade names and domain names; contain hyperlinks that direct the recipient to websites controlled by WORLD AVENUE or its agents, and/or contain hyperlinks that direct the recipient to web servers containing image or text files provided by WORLD AVENUE.

68. Exhibit 23 is an Affidavit of Paul A. Wagner accurately listing the trade names and/or domain names of WORLD AVENUE that appeared in the EMAILS AT ISSUE identified to date and stating the number of emails containing each name. Each of these names identifies with a unique website or domain name that belongs to WORLD AVENUE.

69. Defendant JI directed, participated in, stood to derive revenue, and actually derived revenue, as a result of the transmission of the EMAILS AT ISSUE. JI communicated with the managing agents and employees of WORLD AVENUE, and those entities under contract to him, on each of the dates of transmission of the EMAILS AT ISSUE, beginning on or

before July 20, 2004 and continuing up to the present, in furtherance of the campaigns to transmit those emails.

70. These communications occurred via email, text message and telephone. JI sent and received funds to and from these entities and persons, pertaining to the email campaigns. JI also directed others to conduct the activities alleged in this paragraph on his behalf, and in his stead, and ratified those activities by endorsing, approving and confirming them afterward.

VI. FALSITY AND DECEPTION

71. The EMAILS AT ISSUE sent by the Defendants have multiple elements of falsified, misrepresented, and forged information contained in or accompanying the email headers. These categories correspond directly to conduct prohibited in the MD-CEMA and the FL-CEMA. These categories are as follows :

- Deceptive Subject Lines
- Deceptive Sender Names
- Falsely Registered Sending Domain Names
- Deceptive Information about Origin or Transmission Path in Message Body
- Forged Mailserver Information

A. Deceptive Subject Lines

72. The Federal Trade Commission accurately reported that of the Spam containing signs of falsity in the "Subject:" line, nearly one-third contained a line that bore no relationship to the content of the message and nearly forty-two percent misrepresented that there was a personal or business relationship with the recipient. See "False Claims in Spam: A report by the FTC's Division of Marketing Practices." FTC, April 30, 2003, p. 6, available at http://www.ftc.gov/reports/spam/030429spamreport.pdf (last visited 12/21/08).

73. In addition, DEFENDANTS' emails contained false and/or misleading information in the subject lines, including that which has the capacity, tendency, or effect of deceiving the recipient. This includes, for example, "win a free gift card" when a purchase is required. The subject lines of Defendants' emails were designed by Defendants and/or their agents in attempt to deceive the recipient. (See Exhibit 34C.)

74. DEFENDANTS' failure to include any caveats to the use of the word "free" in the subject line is blatantly deceptive.

75. The Federal Trade Commission has created specific guidelines for advertisers' use of the word "free." See Exhibit 35.

76. To avoid falsity or deception, any contingencies to the "Free" offer should be set forth clearly and conspicuously at the outset of the offer so as to leave no reasonable probability that the terms of the offer might be misunderstood. See Federal Trade Commission, FTC Guide Concerning Use Of The Word "Free" And Similar Representations 16 C.F.R. § 251.1(c), available at http://www.ftc.gov/bcp/guides/free.htm.

77. The FTC's general rules are expressly applicable to the Internet and email advertising. See Federal Trade Commission, Dot Com Disclosures at *5, available at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf

B. Deceptive Sender Names

78. DEFENDANTS used fictitious names and/or used email addresses from individuals without their permission in the EMAILS AT ISSUE.

79. In addition, the EMAILS AT ISSUE contained false and/or misleading header information in the “From:” line about the origin and/or the transmission path of the email because each email contained one or more fictitious, false and/or misleading names and/or email addresses in the "From:" lines. For example, Exhibit 36B falsely states that the email was sent from "Sam's Club".

80. On April 14, 2005, WORLD AVENUE sent hundreds of emails to BSI promoting a "free gift card" on behalf of Consumer Incentive Promotions purporting to be from over 500 different people. Exhibit 34C is one such email. The "From:" line in each message contained a unique and random display name (a.k.a. quoted name) that was gibberish.

81. By varying the domain names where it appears that an email originates, DEFENDANTS could avoid spam filters that may focus on bulk mailings while increasing the chance that the Spam will reach its intended audience.

82. Exhibit 34C indicates that the sender used a computer at IP address 204.13.17.33, but the machine at that address incorrectly identified itself as "mailpool.jriad.info," which the bulk emailer's own DNS server confirmed did not resolve to that IP address. This false identification masks the identity of the sender of the emails and prevents the recipient from finding or contacting the sender.

C. Falsely Registered Sending Domain Names

83. DEFENDANTS and/or their agents sent "Incentive Awards" emails to Plaintiff BSI that included domain names which were registered to false and/or non-existent entities, as well as entities using false addresses and/or false telephone numbers.

84. DEFENDANTS registered hundreds of throw-away domain names in order to send the EMAILS AT ISSUE to BSI. DEFENDANTS also used fake names, addresses and/or proxy services in the Whois Registry for the domain to conceal its identity.

85. The URL combinations used in the thousands of EMAILS AT ISSUE redirect to websites controlled by WORLD AVENUE.

D. Deceptive Information about Origin or Transmission Path in Message Body

86. The EMAILS AT ISSUE contained false or misleading information about the origin or the transmission path of the commercial electronic mail in the message body itself. Some of the EMAILS AT ISSUE falsely claim prior relationships with the recipient and/or that the recipient had requested the email. For example, Exhibit 34A, falsely states in part that "you were a official member of one of our range of online services."

87. Exhibit 34C states the following in the message body: "If you no longer wish to receive Consumer Incentive Promotions emails, ... write us at: Consumer Incentive Promotions, 14545 J Military Tr. #189, Delray Beach, FL 33484, USA." This implies that Plaintiff once wished to receive Consumer Incentive Promotions emails, which is false.

88. In addition, "Consumer Incentive Promotions" is not a corporate or trade name recognized by the state of Florida.

E. Forged Mailserver Information

89. Standard email transmission protocol requires that the HELO/EHLO line in the email headers identify the sending mailserver domain name. See Exhibit 36, "National Do Not

Email Registry: A Report to Congress." FTC, June 2004, Section III (pp. 3-13), available at http://www.ftc.gov/reports/dneregistry/report.pdf (last visited 12/21/08).

90. When an email arrives, the transmitting computer sends a "HELO," which is a parameter typically showing the computer's name and/or IP address so as to identify to the recipient computer who is sending the email and where it came from. In the case of thousands of these emails, the identities of the transmitting computers given in the HELO did not match the IP addresses of the transmitting computers.

91. One example of falsity is shown in Exhibit 34A, in which the sender of the email used a computer at IP address 63.243.148.219. The sending machine identified itself as "PRODUCTTESTERSWEWANT.INFO", which DEFENDANTS' own DNS server confirmed resided at a completely different IP address. This false identification was designed to mask the identity of the sender of the emails and to make it more difficult, if not impossible, to find or contact the sender.

92. Plaintiff alleges the EMAILS AT ISSUE contained false and/or misleading header information about the origin or the transmission path of the email. This includes, for example, that the email arrived at BSI's servers containing or accompanied by false information concerning the identities of the computers sending the emails.

VII. MD-CEMA

93. DEFENDANTS violated the Maryland Commercial Electronic Mail Act, (MD-CEMA) §14-3001 et seq. of the Commercial Law Article of the Annotated Code of Maryland,

by initiating, conspiring to initiate, and/or assisting in the transmission to Plaintiff BSI of commercial electronic mail having one or more of the following characteristics:

i) used a third party's Internet domain name or electronic mail address without that third party's permission;

ii) contained false or misleading information about the origin of the email or the path by which the email was transmitted; or;

iii) contained false or misleading information in the subject line.

94. The false or misleading information in the electronic mail messages had the capacity, tendency, or effect of deceiving the recipient.

95. DEFENDANTS initiated, conspired to initiate, and/or assisted in the transmission of the emails at issue to recipients in Maryland, including Plaintiff.

96. The EMAILS AT ISSUE advertised property, goods or services for sale or lease, to person in Maryland. DEFENDANTS derived substantial revenue as a result of these email messages to recipients in Maryland. By this conduct, DEFENDANTS solicited sales and conducted business in Maryland on a regular basis, engaged in a persistent course of conduct in Maryland, and availed themselves of the protection of the laws of this State.

97. DEFENDANTS planned, prepared, designed, executed, approved, modified, condoned and ratified the sending of the emails referenced above.

98. DEFENDANTS paid others for services related to the transmissions, and received payment from advertisers and others for DEFENDANTS' services related to the transmissions. DEFENDANTS, either directly or indirectly, caused products and services to be

sold and/or delivered as a result of the transmissions. DEFENDANTS tracked the results of the transmissions and all related services, sales and commissions. All of these activities generated records that identify the participants in these activities, and the related times, dates, quantities and payment amounts.

99. All of the conduct alleged above was performed either directly by DEFENDANTS or by persons acting as their agents. All persons who participated in the events alleged above acted as agents for Defendants. All DEFENDANTS (including Does 1-20) authorized, participated in, acquiesced to, consented to and/or were the agents of the other DEFENDANTS in the acts alleged, and initiated, conspired, assisted, participated in, or otherwise encouraged the conduct alleged in furtherance of one or more conspiracies to initiate the emails. The transmissions of the emails identified herein were actions that each of the DEFENDANTS authorized, controlled or directed, or had the ability to authorize, control or direct, and were actions for which each of the DEFENDANTS is liable.

100. As a recipient of the emails at issue, under MCEMA §14-3003(1) Plaintiff BSI is entitled to the greater of $ 500 per violation or actual damages, plus attorney's fees and costs. As an interactive computer service provider, under §14-3003(3) Plaintiff is entitled to the greater of $1,000 per violation or actual damages, plus attorney's fees and costs.

VIII. FL-CEMA

101. FL-CEMA provides in relevant part as follows:

668.603 Prohibited activity.

A person may not:

(1) Initiate or assist in the transmission of an unsolicited commercial electronic mail message from a computer located in this state or to an electronic mail address that is held by a resident of this state which:

(a) Uses a third party's Internet domain name without permission of the third party;

(b) Contains falsified or missing routing information or otherwise misrepresents, falsifies, or obscures any information in identifying the point of origin or the transmission path of the unsolicited commercial electronic mail message;

(c) Contains false or misleading information in the subject line; or

(d) Contains false or deceptive information in the body of the message which is designed and intended to cause damage to the receiving device of an addressee or of another recipient of the message. However, this section does not apply to electronic mail messages resulting from or created by a computer virus which are sent or retransmitted from a computer or other electronic device without the senders knowledge or consent.

* * *

668.606 Remedies.

* * *

(3) A prevailing plaintiff in an action filed under this part is entitled to:

(a) An injunction to enjoin future violations of s. 668.603.

(b) Compensatory damages equal to any actual damage proven by the plaintiff to have resulted from the initiation of the unsolicited commercial electronic mail message or liquidated damages of $500 for each unsolicited commercial electronic mail message that violates s. 668.603.

(c) The plaintiffs attorneys fees and other litigation costs reasonably incurred in connection with the action.

Violations of Section 668.603.

(1) A violation of s. 668.603 shall be deemed an unfair and deceptive trade practice within the meaning of part II of chapter 501. In addition to any remedies or

penalties set forth in that part, a violator shall be subject to the penalties and remedies provided for in this part.

(2) The remedies of this part are in addition to remedies otherwise available for the same conduct under federal or state law.

102. The allegations in the preceding paragraphs of this complaint are hereby incorporated by reference.

103. DEFENDANTS violated FL-CEMA by initiating or assisting in the transmission of unsolicited commercial electronic mail messages, including the emails at issue, from computers located in Florida. Each of these emails contained falsified or missing routing information or otherwise misrepresented, falsified or obscured information in identifying the point of origin or the transmission path of the unsolicited commercial electronic mail message; and contained false and misleading information in the subject lines, and contained false and deceptive information in the body of the messages, designed and intended to cause damage to the receiving device of an addressee or of another recipient of the message.

104. In particular, DEFENDANTS caused email messages to be sent as described in the preceding paragraphs of this complaint.

IX. COUNTS

Count I - MCEMA

105. The allegations above are incorporated by reference.

106. DEFENDANTS initiated, conspired in the initiation, and assisted in the transmission, of the EMAILS AT ISSUE in this suit.

Count II - FL CEMA

107. The allegations above are incorporated by reference.

108. DEFENDANTS initiated, conspired in the initiation, and assisted in the transmission, of the EMAILS AT ISSUE in this suit.

PRAYER FOR RELIEF

Plaintiff seeks judgment as follows:

A. against all DEFENDANTS, jointly and severally, under §14-3003(1) of MD-CEMA, Plaintiff BSI seeks judgment in the amount of $ 500 for each of the commercial electronic mail messages at issue, in an aggregate amount of not less than Thirty-Four Million Dollars ($34,000,000);

B. against all DEFENDANTS, jointly and severally, under §14-3003(3) of MD-CEMA, Plaintiff BSI seeks judgment in the amount of $1,000 for each of the commercial electronic mail messages at issue, in an aggregate amount of not less than Sixty-Eight Million Dollars ($68,000,000), in addition to the damages sought in paragraph (a) above;

C. Plaintiff seeks an order enjoining DEFENDANTS under Md. Code Ann., Com. Law. MD-CEMA from making any false or misleading statements in commercial emails, and from engaging in any further conduct in violation of MD-CEMA.

D. Under MD-CEMA, against all DEFENDANTS, Plaintiff BSI seeks an award of attorney's fees, and the reasonable costs of this litigation.

E. against all DEFENDANTS, jointly and severally, under FL-CEMA, Plaintiff BSI seeks judgment in the amount of $ 500 for each of the commercial electronic mail messages at

issue, in an aggregate amount of not less than Thirty-Four Million Dollars ($34,000,000), in addition to the damages sought in the paragraphs above;

F. Plaintiff seeks an order enjoining DEFENDANTS under FL-CEMA 668.606(3)(a) from making any false or misleading statements in commercial emails, and from engaging in any further conduct in violation of FL-CEMA.

G. Under FL-CEMA, against all DEFENDANTS, Plaintiff BSI seeks an award of attorney's fees, and the reasonable costs of this litigation.

H. Plaintiff BSI seeks damages for any continuing violations up to the time of entry of judgment, not limited to the quantities of violations known as of the filing of this complaint, and such other and further relief as the Court deems appropriate.

Respectfully submitted,

/s/ 12/22/08
Stephen H. Ring Date
STEPHEN H. RING, P.C.
20300 Seneca Meadows Parkway, Suite 200
Germantown, Maryland 20876
MD Bar Id. No. 04731764; USDC, MD: #00405
Telephone: 301-540-8180

/s/ 12/22/08
Michael S. Rothman Date
401 E. Jefferson Street
Suite 201
Rockville, MD 20850
Phone: (301) 251-9660
Fax: (301) 251-9610

Attorneys for Plaintiff

Jury Demand

Plaintiff requests a trial by jury as to all issues so triable.

/s/
Michael S. Rothman

EXHIBITS LIST

Exhibit 12 - BARRACUDA NETWORKS, BARRACUDA NETWORKS SPAM REPORT at 4 (2007).

Exhibit 13 - Order in Facebook, Inc. v. Guerbuez, et al., Case No. CO8003889 HRL (U.S. District Court, Northern District of California, November 10, 2008).

Exhibit 14 - USDOJ Press Release: "Brooklyn Man Sentenced to 30 months in Prison in Massive AOL Spam Scheme."

Exhibit 15 -- USDOJ Press Release, October 12, 2007: "Two Men Sentenced For Running International Pornographic Spamming Business."

Exhibit 16A -- FTC Press Release: "ValueClick to Pay $ 2.9 Million to Settle FTC Charges."

Exhibit 16B -- FTC, "Major Online Advertiser Settles FTC Charges. "Free" Gifts Weren't Free; Settlement Calls for $650,000 Civil Penalty," Nov. 28, 2007.

Exhibit 17 - "News Release: Internet Company Sued for Deceptive Advertisements of "Free" Gifts." pp. 1-2.

Exhibit 18 - Better Business Bureau Company Report for Niutech, LLC listing alternative dba's.

Exhibit 19 - Lazarus, David, "No Such Thing as a free laptop." San Francisco Chronicle, June 15, 2007

Exhibit 20 -- RipOff Report on World Avenue, listing URLs and fictitious business names.

Exhibit 21 -- Royal Bank of Canada Capital Markets report on ValueClick & Lead Generation, April 26, 2007.

Exhibit 22A -- http://www.theuseful.com/site/aboutus.html, captured on 12/19/2008.

Exhibit 22B – FTC, Report to Congress, "A CAN-SPAM Informant Reward System," Sept. 2004, excerpt.

Exhibit 23 -- Affidavit of Paul A. Wagner Regarding Count of Emails Containing Certain Business Names and Domain Names, Dec. 22, 2008.

Exhibit 24 -- www.SuperbRewards.com and other World Avenue destination web pages (landing pages).

Exhibit 25 -- Declaration of Homer Appleby, Esq., Oct. 19, 2006.

Exhibit 26 - Whois registration lookups of World Avenue domain names, June 2007.

Exhibit 27 – Terms Of Service of World Avenye web sites, April 19, 2007.

Exhibit 28 – Florida Secretary of State corporate listing for Net Radiance LLC, 12/19/2008.

Exhibit 29 -- Florida Secretary of State corporate listing for World Avenue Holdings, LLC, 12/19/2008.

Exhibit 30 -- Florida Secretary of State corporate listing for World Avenue U.S.A., LLC, 12/19/2008.

Exhibit 31 -- www.superbrewards.com image refers to theuseful.com, 6/19/2007.

Exhibit 32 – Florida Attorney General, "McCollum's CyberFraud Task Force Reaches $1 Million Agreement with Company over Internet Marketing Guidelines," January 16, 2008.

Exhibit 33 -- DMA publication, "DMA Ethics Committees Call Attention to Non-Compliant Companies," August 28, 2007.

Exhibit 34A -- sample spam--$250 gift card--prefer Startbucks or Dunkin Donuts.

Exhibit 34B -- sample spam--Sams Club gift card.

Exhibit 34C -- sample spam--$250 gift card--prefer Startbucks or Dunkin Donuts.

Exhibit 34D -- sample spam--Target Gift Card.

Exhibit 35 -- "FTC Guide Concerning Use of the Word "Free" and Similar Representations," (38 Stat. 717, as amended; 15 U.S.C. 41 - 58), [36 FR 21517, Nov. 10, 1971].

Exhibit 36 – FTC, "National Do Not Email Registry -- A Report to Congress," June 2004.